



Legislative Bulletin.....October 17, 2007

Contents:

H.R. 3773— RESTORE Act of 2007

Summary of the Bill Under Consideration Today:

Total Number of New Government Programs: 0

Total Cost of Discretionary Authorizations: Such sums as appropriated

Effect on Revenue: \$0

Total Change in Mandatory Spending: 0

Total New State & Local Government Mandates: 0

Total New Private Sector Mandates: 1

Number of Bills Without Committee Reports: 0

Number of Reported Bills that Don't Cite Specific Clauses of Constitutional Authority: 0

H.R. 3773— RESTORE Act of 2007 (*Conyers, D-MI*)

Order of Business: The bill is scheduled to be considered on Wednesday, October 17th, subject to a closed rule ([H.Res. 746](#)). The rule:

- waives all points of order against *consideration* of the bill except those for earmarks and PAYGO;
- provides that in lieu of the amendments recommended by the Judiciary Committee and the Intelligence Committee, an amendment in the nature of a substitute, as modified by a self-executing amendment, shall be considered as adopted;
- waives all points of order against the bill itself, as amended, except for the earmark point of order; and

- allows one motion to recommit, with or without instructions.

Summary: H.R. 3773 would amend the Foreign Intelligence Surveillance Act of 1978 (FISA) and provide the U.S. intelligence community the authority to conduct foreign communication surveillance through December 31, 2009. The bill would require that the government receive permission from a Foreign Intelligence Surveillance Court (FISC) to conduct surveillance on persons who are “reasonably believed” to be non-U.S. citizens communicating outside of the U.S. The bill would also establish new guidelines, procedures, and audit requirements for agencies gathering foreign intelligence. The provisions of the bill are as follows:

Sec. 2 — Clarification of Electronic Surveillance of Non-U.S. Persons outside the U.S.

- Provides that a court order is not required to obtain communication between people who are reasonably believed to be located outside the U.S. and are not known to be U.S. citizens or residents for the purpose of collecting foreign intelligence information, regardless of whether the communication passes through the U.S. or the surveillance device is located within the U.S.;
- Requires that if any communication obtained contains at least one party who is a U.S. person or is located in the U.S., the AG will ensure that no contents of any communication shall be disclosed, disseminated, or used for any purpose or retained for more than seven days.

Sec. 3 — Additional Authorization of Acquisitions of Communications of Non-U.S. Persons outside the U.S. Who may be Communicating with Persons inside the U.S

- Allows the Director of National Intelligence (DNI) and the Attorney General (AG), to apply to a FISC judge for an *ex parte* order, or an extension of an order, to authorize electronic surveillance for periods of up to one year, for the purpose of obtaining foreign intelligence information from people reasonably believed to be non-U.S. citizens outside of the U.S.

Note: *Ex parte* means a notice on behalf of one party *without* notice to any other party.

- States that the application for the order is required to include certification from the AG and the DNI that:
 - a) the targets of intelligence acquisition are reasonably believed to be non-U.S. persons outside of the U.S.;
 - b) the acquisition of intelligence involves obtaining the assistance of a communications provider; and
 - c) the purpose of the acquisition is to obtain foreign intelligence information.
- States that the application for the order is required to include a description of:
 - a) procedures that will be used to determine that the targets of the surveillance are non-U.S. persons located outside the U.S.;
 - b) the nature of the information sought;

- c) minimization procedures; and
 - d) guidelines that will be used.
- States that the application for the order is not required to identify the specific facilities, places, premises, or property at which the acquisition of foreign intelligence will be directed.
- Provides that a judge will review and approve the application if the judge finds that:
 - a) the proposed procedures in the application are reasonably designed to determine whether the targets are non-U.S. persons located outside the U.S.;
 - b) the proposed minimization procedures meet the definition under section 101(h); and
 - c) the guidelines ensure that the government obtains an individualized warrant when a significant purpose of the collection is to acquire the communications of a specific United States Person reasonably believed to be inside the United States.
- Directs a judge who is approving an application to issue an order that:
 - a) authorizes surveillance as requested, or as modified by the judge;
 - b) requires a communications service provider (or other person who has lawful authority to access the information or facilities) to furnish the applicant information (upon request) in a manner that will protect the secrecy of the surveillance and produce minimum interference with the services of that provider;
 - c) requires the service provider (upon request of the applicant) to maintain records concerning the acquisition or the aid furnished (under security procedures approved by the AG or the Director of National Intelligence);
 - d) directs the federal government to compensate a person (at the prevailing rate) for providing information or assistance to such an order and to provide a portion of the court order directing compliance to the communications service provider; and
 - e) directs the applicant to follow the minimization procedures as proposed or modified by the court.
- Allows the AG, through the FISA court, to compel a communications service provider to comply with an order.
- Provides that no cause of action shall lie in any court against a communications service provider for complying with an order issued under this section.
- Requires the DNI and the FISA court to retain any order issued under this section for at least ten years.
- Requires the FISA court judge to assess compliance on a quarterly basis with the procedures and guidelines of the surveillance order.

Sec. 4 — Emergency Authorization of Acquisition of Communications of non-U.S. Persons outside the U.S.

- Requires the DNI and the AG to submit an application within seven days of authorizing emergency acquisition of foreign intelligence.
- Allows the DNI and the AG to jointly authorize the emergency acquisition of foreign intelligence for a period of no more than 45 days if:
 - 1) The DNI and AG jointly determine that:
 - a) an emergency situation exists that prohibits acquisition under section 105B;
 - b) the targets of the acquisition are reasonably believed to be non-U.S. persons outside of the U.S.;
 - c) there are reasonable procedures in place to determine that the target of acquisition is a non-U.S. person outside the U.S.;
 - d) the acquisition involves obtaining foreign intelligence from, or with the assistance of, a communications service provider;
 - e) the purpose of the acquisition is to obtain foreign intelligence information;
 - f) minimization procedures meet the definition under 101(h); and
 - g) there are reasonable guidelines designed to ensure that the government obtains an individualized warrant when a significant purpose of the collection is to acquire the communications of a specific United States person reasonably believed to be located inside the United States.
 - 2) The DNI and the AG inform a FISA court judge of any emergency acquisition of foreign intelligence.
- Provides that when the emergency acquisition of foreign intelligence is authorized, the AG may direct a communications service provider to:
 - a) furnish the AG with information, facilities, or technical assistance in a manner that will protect the secrecy of the acquisition and produce minimum interference with the communications service provider; and
 - b) maintain any records concerning the acquisition or aide furnished.

Sec. 5 — Oversight of Acquisitions of Communications of non-U.S. Persons outside the U.S.

- Requires the DNI and the AG to submit each application or order (including certification, purpose, procedures, and guidelines) for acquisition of foreign intelligence under section 105B to the appropriate committee of Congress within seven days.
- Requires the DNI and the AG complete quarterly audits on the procedures and guidelines of every order authorizing the acquisition of foreign intelligence and submit the results to the appropriate committee of Congress, including:
 - a) the number of targets that were later determined to be in the U.S.;
 - b) the number of people in the U.S. whose communications have been acquired under an order;
 - c) the number and nature of reports disseminated that contain information on a U.S. person that was collected under such order; and

- d) the number of applications submitted for electronic surveillance for targets whose communications were acquired under such order.
- Requires the AG to submit the report to the appropriate committees in Congress within 30 days of the completion of an audit.
- Requires the DNI and the AG to submit quarterly compliance reports to the appropriate committees in Congress and the FISA court regarding the acquisition of foreign intelligence, including any non-compliance by:
 - a) an element of the intelligence community with minimization, guidelines or procedures; and
 - b) a person directed to provide information, facilities, or technical assistance.
- Requires the DNI and the AG to submit annual reports to the appropriate committees of Congress containing the number of emergency authorizations of intelligence acquisitions and any incidents of non-compliance with an emergency authorization.

Sec. 6 — Foreign Intelligence Surveillance Court En Banc.

- Allows a FISA court, if it so chooses, to sit *en banc* (the full court, with multiple judges).

Sec. 7 — Foreign Intelligence Surveillance Court Matters

- Increases the number of FISC judges who may hear applications for and grant orders approving electronic surveillance anywhere within the United States.
- Provides that a FISC judge may make a determination to approve, deny, or modify an application approving electronic surveillance within 24 hours of receiving the application.

Sec. 8 — Reiteration of FISA as the Exclusive Means by which Electronic Surveillance May Be Conducted for Gathering Foreign Intelligence Information

- Reiterates that FISA shall be the exclusive means by which electronic surveillance for the purpose of gathering foreign intelligence may be conducted.

Sec. 9 — Enhancement of Electronic Surveillance Authority in Wartime and Other Collection

- Allows the President, through the Attorney General, to authorize electronic surveillance without a court order for no more than 15 days following a declaration of war by the Congress or when the constitutional powers of the President as Commander-in-Chief introduce United States Armed Forces into hostilities pursuant to specific statutory authorization.

Sec. 10 — Audit of Warrantless Surveillance Programs

- Requires the Inspector General of the Department of Justice (DOJ IG) to **complete an audit of all warrantless surveillance conducted on or after September 11, 2001, including the “Terrorist Surveillance Program referred to by the President in a radio address on December 17, 2005”** within 180 days.
- Requires the DOJ IG to submit a report to the Permanent Select Committee on Intelligence and appropriate committees in Congress containing the results of the audit **including all documents procured. The report shall be submitted in unclassified form, but may include a classified annex.**
- Requires the DNI to ensure that the process for granting necessary clearances for the DOJ IG and appropriate staff is done expeditiously.

Sec. 11 — Record Keeping System on Acquisition of Communication of U.S. Persons

- Requires that the DNI and the AG establish and maintain a record-keeping system to keep track of:
 - a) instances where the identity of a U.S. person whose communications were acquired is disclosed by an element of the intelligence community;
 - b) the departments, agencies, and persons to whom such identity information was disclosed.
- Requires the DNI and the AG to submit a report to the appropriate committees of Congress regarding the record-keeping system.

Sec. 12 — Authorization for Increased Resources Related to Foreign Intelligence Surveillance

- Authorizes the appropriation of “such sums as may be necessary” for submitting applications to the FISA courts and fulfilling audit, reporting, and record-keeping requirements.

Sec. 13 — Additional Personnel for Preparation and Consideration of Applications for Orders Approving Electronic Surveillance and Physical Search

- Authorizes the National Security Division of the Department of Justice and the DNI such additional personnel as may be necessary to carry out the prompt and timely preparation, modification, and review of applications under FISA.

Sec. 14 — Document Management System for Applications for Orders Approving Electronic Surveillance

- Requires the AG, in consultation with the DNI and the FISC, to develop a classified document management system that permits the prompt preparation, modification, and review by appropriate personnel of the DOJ, the FBI, the NSA, and other applicable elements of the government of surveillance applications under FISA.

Sec. 15 — Training of Intelligence Community Personnel in Foreign Intelligence Collection Matters

- Requires the DNI and the AG to develop regulations to establish procedures for conducting and seeking approval of electronic surveillance, physical search, and the installation and use of pen registers and trap and trace devices on an emergency basis under FISA.

Sec. 16 — Information for Congress on the Terrorist Surveillance Program and Similar Programs

- Requires the President, within seven days of enactment, to fully inform each member of the Permanent Select Committee on Intelligence of the House and the Senate on:
 - a) the Terrorist Surveillance Program of the National Security Agency; and
 - b) any program in existence from September 11, 2001, that involves the electronic surveillance of United States persons in the United States for foreign intelligence or other purposes, without fully complying with the procedures set forth in FISA.

Sec. 18 — Sunset; Transition Period

- Provides that provisions under this Act are repealed as of December 31, 2009, and that any authorization that was in effect prior to the enactment of this Act shall remain in effect until its expiration or until 180 days after the date of enactment.

The following sections will be re-designated at the appropriate place in the bill:

Certification to Communications Service Providers that Acquisitions are Authorized Under FISA

- Requires an applicant for a FISA surveillance order provide communication service providers with a certification stating that the surveillance is authorized and that all FISA requirements have been met.

Statute of Limitations

- Prohibits a person from being prosecuted, tried, or punished for any FISA related offense unless the indictment is found or the information is instituted no later than ten years after the commission of the offense.

No Rights Under the RESTORE Act for Unlawful Residents

- States that nothing in the Act will prevent lawfully conducted surveillance of or grant any rights to illegal aliens.

Additional Background: FISA was created in 1978 to establish a process for obtaining a court order to conduct foreign intelligence surveillance within the United States. Due to dramatic changes in telecommunications technology since then, FISA now frequently requires

government officials to obtain a court order to gather information on suspected terrorists and various other foreign intelligence targets located overseas. Federal law has not historically restricted law enforcement officials or intelligence agents from monitoring overseas communications, and this bill is intended to address these concerns.

In April, 2007, Director of National Intelligence Mike McConnell came to Congress with [a proposal](#) to extend and modernize FISA in order to address changes in telecommunications technology. H.R. 3773 differs greatly from Director McConnell's original proposal by requiring professionals in the intelligence community to obtain a FISC warrant or court order before conducting surveillance overseas. The underlying legislation also diverges from McConnell's proposal by not granting protection from liability to communication providers that helped intelligence agencies gather information following 9/11.

In August, two short term extensions of FISA were considered in order to extend surveillance authority and modernize overseas communication monitoring. H.R. 3356, the Improving Foreign Intelligence Surveillance to Defend the Nation and the Constitution Act of 2007, a Democrat proposal that contained many similar provisions to the underlying bill, was defeated on August 3, 2007 while under suspension by a vote of [218 – 207](#). S. 1927, the Protect America Act of 2007 (PAA), a Republican sponsored, bi-partisan bill that allowed intelligence professionals to gather overseas information without a court order, passed the House by a vote of [227 – 183](#). The PAA, which will sunset 180 days after its enactment, would be repealed and replaced by the H.R. 3773. During committee consideration of H.R. 3773, an amendment in the nature of a substitute was offered to permanently extend the PAA and was defeated by a vote of 14 – 21.

Possible Conservative Concerns: Some conservatives may be concerned that H.R. 3773 would impede the efforts of intelligence professionals and endanger the country's security by requiring a court order to conduct electronic surveillance on a person reasonably believed to be a non-U.S. citizen operating outside of the U.S. Further, some conservatives may also be concerned that H.R. 3773 would require court approval to obtain foreign intelligence in non-emergency situations, which may hinder our ability to properly collect and respond to terrorist threats and pertinent intelligence.

Some conservative may also be concerned that H.R. 3773 omits language that would protect communication providers that have assisted the intelligence community in the past from legal liability. In addition, conservatives may be concerned that the bill would sunset on December 31, 2009, leaving the intelligence community in the current less-than-desirable situation in just two years.

The Judiciary Committee's dissenting views, in [House Report 110 – 373, Part I](#), as well as the Permanent Committee on Intelligence's dissenting views, in [House Report 110 – 373, Part II](#), and the Administration, in its [Statement of Administration Policy](#) (SAP), have expressed a number of additional concerns, including:

- The extensive oversight provisions imposed by the bill, such as audit and reporting requirements, may detract from the already scarce resources of the nation's intelligence community.
- The bill may infringe American's civil liberties by creating and maintaining a single database that lists all Americans who have been identified in foreign intelligence information and whose identity has been disclosed to other agencies regardless of whether or not they have been suspected as a terrorist or spy.
- The bill may further hamper the intelligence community from doing its job by giving FISC judges the power to assess compliance with the court order every 120 days with no restrictions on the process for review or remedy.

Committee Action: H.R. 3773 was introduced on October 9, 2007, and was referred to the Committee on the Judiciary, and the Committee on Intelligence (Permanent Select). The following day, a mark-up was held in the Judiciary Committee. The bill was reported out of the committee, as amended, by a vote of 20 – 14.

On October 12, 2007 the Judiciary Committee reported [House Report 110 – 373, Part I](#), and the Committee on Intelligence (Permanent) reported [House Report 110 – 373, Part II](#).

Administration Position: According to a [SAP](#) released by the Administration on Tuesday, October 16, 2007, “if H.R. 3773 is presented in its current form to the President, **the Director of National Intelligence and the President's other senior advisers will recommend that he veto the bill.**”

Cost to Taxpayers: CBO finds that “several sections of the bill would, if implemented, increase discretionary costs. However, CBO does not have access to the information necessary to estimate the impact on the budget of implementing H.R. 3773.” All funds for H.R. 3773 would be subject to appropriation.

Does the Bill Expand the Size and Scope of the Federal Government? Yes, the bill alters current regulations and requirements regarding electronic surveillance and foreign intelligence information gathering.

Does the Bill Contain Any New State-Government, Local-Government, or Private-Sector Mandates?: Yes, the bill contains state and local government mandates by preempting state and local liability laws by protecting certain individuals who comply with federal requests for information from lawsuits.

H.R. 3773 also contains private sector mandates because it would compel communication services providers to assist the government with electronic surveillance.

Does the Bill Comply with House Rules Regarding Earmarks/Limited Tax Benefits/Limited Tariff Benefits?: The Judiciary Committee, in [House Report 110—373](#), asserts that, “H.R. 3773 does not contain any congressional earmarks, limited tax benefits, or limited tariff benefits as defined in clause 9 of rule XXI.”

Constitutional Authority: The Judiciary Committee, in [House Report 110—373](#), cites constitutional authority in Article I, Section 8, Clause 1 (relating to the congressional power to promote the general welfare of the United States) and Clause 18 (relating to the congressional power to make all laws necessary and proper for carrying into Execution the foregoing Powers).

RSC Staff Contact: Andy Koenig; andy.koenig@mail.house.gov; 202-226-9717.
